IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

IN RE: BLACKBAUD, INC., CUSTOMER DATA BREACH LITIGATION	Case No.: 3:20-mn-02972-JMC MDL No. 2972 **CASE MANAGEMENT ORDER NO. 7B (PLAINTIFFS' DEFENDANT FACT SHEET)**

THIS DOCUMENT RELATES TO: ALL ACTIONS

This matter is before the court on Defendant Blackbaud, Inc.'s ("Defendant") objection to Plaintiffs' Defendant Fact Sheet. (ECF No. 48 at 1-4.) Specifically, Defendant objects to Plaintiffs' request that Defendant identify its customers who were notified of a data security breach of Defendant's systems. (*Id.*) For the reasons set forth below, the court overrules Defendant's objection to the request.

I. BACKGROUND

Defendant is a cloud software company that sells customer data collection and maintenance platforms to organizations such as hospitals, schools, museums, and foundations. (ECF No. 48 at 3.) Defendant's customers use Defendant's administrative, fundraising, and financial management software solutions to collect and manage data from their own customers. (*Id.*)

This multidistrict litigation involves numerous purported class actions arising out of an alleged ransomware attack and data security breach of Defendant's systems from February 2020 through May 2020 (the "Security Incident"). (ECF No. 1 at 1-2.) Plaintiffs allege that the Security Incident compromised the personal information of millions of consumers who interacted with

organizations that utilized Defendant's cloud software and services. (*Id.*) In other words, they claim that the Security Incident exposed the personal information of Defendant's customers' customers. The cases were transferred to this court for consolidated pretrial proceedings by the United States Judicial Panel on Multidistrict Litigation on December 15, 2020. (*Id.* at 1-4.)

On February 3, 2021, the court directed the parties to exchange their final fact sheets by March 10, 2021. (ECF No. 23 at 2-3.) After receiving Plaintiffs' Defendant Fact Sheet, Defendant objected to Plaintiffs' request that Defendant identify its customers who were notified of the Security Incident. (ECF No. 48 at 1-4.) The parties presented their respective positions on the dispute to the court in a Joint Letter submitted on March 12, 2021 and at the Second Case Management Conference on March 19, 2021. (*Id.*; ECF No. 52.)

II. LEGAL STANDARD

"The Federal Rules of Civil Procedure, along with the court's inherent power, provide ample authority for early and ongoing control of discovery in complex litigation." MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.4 (2004). The general principle governing the scope of discovery stated in Federal Rule of Civil Procedure 26(b)(1) permits discovery of matters, not privileged, "relevant to the claim or defense of any party." *Id.* at § 11.41 (citing FED. R. CIV. P. 26(b)(1)). However, Rule 26(b)(2) directs the court to limit the frequency and extent of use of the discovery methods permitted by the rules in order to prevent "unreasonably cumulative or duplicative" discovery and discovery for which "the burden or expense . . . outweighs its likely benefit, taking into account the needs of the case . . . the importance of the issues at stake . . . and the importance of the proposed discovery in resolving the issues." *Id.* (citing FED. R. CIV. P. 26(b)(2)).

"Prior to class certification under Rule 23, discovery lies entirely within the discretion of the [c]ourt." *Artis v. Deere & Co.*, 276 F.R.D. 348, 351 (N.D. Cal. 2011) (citing *Vinole v. Countrywide Home Loans, Inc.*, 571 F.3d 935, 942 (9th Cir. 2009)). Thus, pre-certification discovery may be targeted at "information that might facilitate settlement negotiations or provide the foundation for a dispositive motion[.]" MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.422 (2004).

III. ANALYSIS

Defendant claims Plaintiffs' request is improper because it seeks information that is "irrelevant to the threshold issue of jurisdiction" and is "overbroad and unduly burdensome at this stage of the proceedings." (ECF No. 48 at 2.) The court disagrees.

First, Plaintiffs' request is highly relevant to the current sequence of litigation addressing "jurisdiction, standing, forum selection, and other procedural grounds[.]" (ECF No. 23 at 4.) In order to establish standing, a plaintiff must have: "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016).

Here, the identities of Defendant's customers who were notified of the Security Incident will allow the court to determine whether the disclosure of putative class representatives' personal information is "fairly traceable" to Defendant's conduct. After the Security Incident occurred, putative class representatives received data breach notification letters from various organizations informing them that their personal information had been compromised in a data breach. (ECF No. 48 at 3.) However, some of the data breach notification letters do not explicitly mention whether their personal information was exposed as result of the Security Incident or whether the organization is or was a customer of Defendant. (*Id.*) Thus, disclosure of the identities of

Defendant's customers will allow Class Counsel to determine whether putative class representatives received data breach notification letters from one of Defendant's customers. If putative class representatives received letters from organizations unrelated to Defendant and their personal information was disclosed as a result of a *different data breach*, they will be unable to establish the causation element of standing for this case and would not be appropriate putative class representatives. Such information would also preempt unnecessary motions to dismiss on this issue.

Defendant asserts that the "law is quite clear that while discovery related to putative class members may be relevant to class certification, it is generally not relevant to other pre-certification issues." (*Id.* at 2.) However, the cases it cites in support of that proposition are inapplicable to the scenario currently before the court. Each of the cases cited by Defendant limited pre-certification discovery of the names and contact information of putative class members out of concern that plaintiffs' attorneys may be seeking such information to identify potential new clients. *See In re: Pella Corp. Architect & Designer Series Windows Mktg., Sales Practices & Products Liab. Litig.*, No. 2:14-MN-00001-DCN, 2014 WL 12622421 (D.S.C. Nov. 20, 2014); *Swelnis v. Universal Fid. L.P.*, No. 2:13-CV-104-PRC, 2014 WL 1571323 (N.D. Ind. Apr. 17, 2014); *Charles v. Nationwide Mut. Ins. Co.*, No. 09-CV-04, 2010 WL 7132173 (E.D.N.Y. May 27, 2010); *Dziennik v. Sealift, Inc.*, No. 05 CV 4659, 2006 WL 1455464 (E.D.N.Y. May 23, 2006). In contrast, the discovery request at issue here does not concern the names and contact information of potential class members. Instead, it seeks the identities of organizations that connect putative class members to Defendant and the Security Incident. Accordingly, the information would be used to confirm whether putative class representatives were actually impacted by the Security Incident rather than to solicit new class members.

Second, Plaintiffs' request is not overly broad or unduly burdensome. Plaintiffs already tailored their request since they "initially requested that [Defendant] provide a list of all individuals whose private information was exposed (by category) and agreed to limit their request in an effort to limit the number of issues the [c]ourt would need to decide at the outset of the litigation." (*Id.* at 4.) Defendant's proposed Plaintiff Fact Sheet also asks each putative class representative to "[i]dentify all Blackbaud customers to whom [they] provided protected information."[1] The court will not permit Defendant to limit Plaintiffs' discovery of Defendant's relationships with Defendant's customers when Defendant seeks discovery of putative class representatives' relationships with Defendant's customers. Furthermore, the request will not impose an unreasonable burden on Defendant because Defendant recently notified its affected customers of the Security Incident. (*Id.* at 3.)

IV. CONCLUSION

For the foregoing reasons, the court overrules Defendant's objection to Plaintiffs' Defendant Fact Sheet and its request that Defendant identify its customers who were notified of the Security Incident.

IT IS SO ORDERED.

J. Michelle Childs

United States District Judge

April 7, 2021
Columbia, South Carolina

[1] Defendant attached its proposed Plaintiff Fact Sheet as an exhibit to the status letter it emailed to the court after the First Case Management Conference on January 29, 2021.